Eduonix

Penetration Test Report

Penetration Test Report

Version: **1.0**
Date: 07/08/2014
Prepared by: Eduonix
Classification: Confidential

Document History and Distribution

1. Version History

Version #	Date	Description	Author
V1.0	07/08/2014	First draft	Eduonix

2. Distribution

Recipient Name	Organisation	Distribution Method
Eduonix clients	Many	FTP

CONTENTS

.

1. SUMMARY

Eudonix has been contracted to perform a penetration test against company X's inter-company networks and external web presence. It was determined that their internal network had minimal possible external access due to strict firewall rules and private networks being non-internet connected.

1.1 Objectives

The test was conducted in a manner that replicated an attack by a malicious party attempting to;

- Gain remote system access
- The impact of a breach
  - Identify what confidential information can be accessed
  - The integrity of the companies systems
  - The service availability during the breach

All tests were performed within the governance outlined in NIST SP800, ideally the results of this test will be used to guide company X through future improvements. All tests were performed with strict acceptance by company X.

While conducting the review, a vulnerability was found in the OpenVPN version running on one of the companies external servers. After exploiting this vulnerability, we were able to footprint the entire connected internal network, as well as gain access to a NFS share holding confidential documents.
We were able to escalate to root privileges on an adjoining wordpress server used to serve the company intranet. This would place the entire network under the control of the attackers.

We also noticed a postgresql database containing door records of employees entering the building. This also had plain text information stored to give terminal access to the door security systems. This would allow us to unlock/lock the main security door on demand.

1.3 Scope

External presence

Entire internal network

2. TEST ITEMS

- *Test plan*
- *VA plan*
- *VA execution*

3. APPROACH

Vulnerability analysis was previously conducted on this system, the results of which were taken into consideration when selecting attack vectors for the target system.

- Perform scans of internal and external systems
- Manual investigation of results
- Rank vulnerabilities based on severity
- Perform further research, indicating development activities required to rectify issues
- Recommend immediate solution
- Knowledge transfer

3.1 Resources

Network plan, provided by company X (IP-PLAN.XLS)

3.2 Schedule

Pending completion of tests, schedule is due to end on 13/08/2014, starting on 08/08/2014

4. ENVIRONMENTAL REQUIREMENTS

(Test environment must be segregated from any live system, because of the nature of the tests they may be intrusive and cause network disruption without warning. Therefore we cannot guarantee uptime of any service in the same environment during this time.

4.1 Hardware

Rasperry Pi – Acting as proxy

4.2 Software

Kali
Metasploit
Nessus

4.3 Security

Security will be performed in isolation, requires metasploit framework community edition.

4.5 Publications

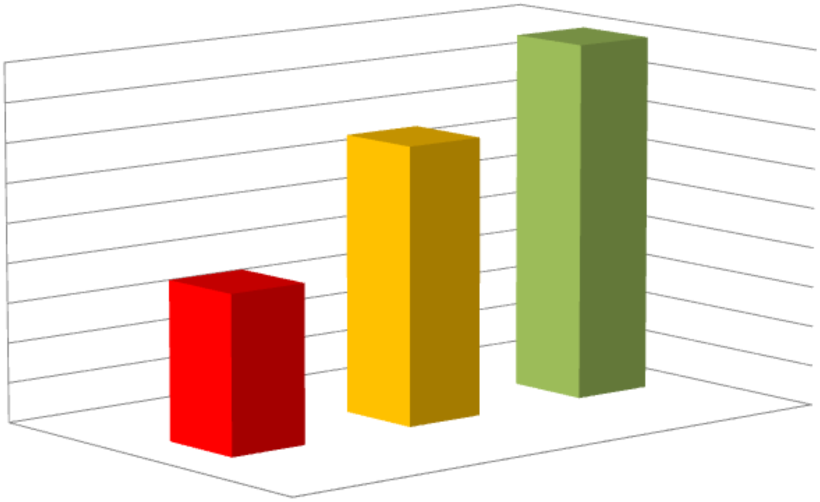
Software test plan
Software test coverage report
Software Pentest report
Software test case raw data

4.6 Risks and Assumptions

Due to storage requirements, the maximum backup we can test is 100GB, it is likely that backups will far exceed this in the field.

.

4. RESULTS & RECCOMMENDATIONS



Finding	Low	Medium	High	Comments

There are three areas that need to be addressed as a result of the internal scan:
system hardening, patch management, and user account management. Each one of these areas should be first addressed at the Corporate Security Policy. Before
procedures can be defined to address the corporate security policies, high-level
solutions will be defined that address each of the three findings. Solution sets will
then be listed and mapped to each finding area.

Approved by _______________ Date__/__/____